REMARKS

The Applicants request reconsideration of the rejection.

Claims 1 and 28 remain pending.

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. Correspondingly, claims 1, 3 and 28 stand rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. Specifically, the Examiner finds a lack of support for the claimed "a table of candidates of disturbance data XI" (claim 1) and "a table of candidate pairs of disturbance data XI and disturbance data XO." The Applicants traverse as follows.

Specification support for "a table of candidates of disturbance data XI" of claim 1 at page 35, line 10 – page 37, line 13 of the present specification. In the embodiment described there, X1i is disturbance data and X1o is processed disturbance data. Page 35, lines 10-12 state, "Fig. 11 is a diagram showing a data flow in a typical technique to generate the X1i disturbance data 1103 and the X1o processed disturbance data 1105". An example of a table holding such candidates is shown in Fig. 55, including the X1i disturbance data and the X1o processed disturbance data (see also the specification at page 37, lines 7-13 which state, "The table includes typical disturbance data X1i and typical processed disturbance data X1o"). Claim 28 is similarly supported.

Claims 1, 3 and 28 stand rejected under 35 U.S.C. §112, second paragraph, as set forth on pages 7-9 of the Office Action. The Applicants have amended claims 1 and 28 to address the Examiner's concerns. Claim 3 has been canceled.

Claims 1, 3 and 28 stand rejected under 35 U.S.C. §103(a) as being unpatentable over the Applicants' Admitted Prior Art (AAPA) in view of Jaffe et al., U.S. Patent No. 6,510,518 (Jaffe). The Applicants traverse as follows.

The currently amended claim 1 has the following features: (a) a table of candidates of disturbance data XI which maintain a constant Hamming weight before and after processing said disturbance data XI with said predetermined processing OP1, (b) a selector for selecting one of disturbance data XI from said table, and (c) a disturbance-data-processing means for performing said predetermined processing OP1 by using said disturbance data XI selected by said selector in order to generate a disturbance data XO.

The embodiment set forth in claim 1 prevents the Hamming weight of data for disturbance from becoming equal to 0 or 8 by using the first disturbance data selected by the above-said process (b) and the second disturbance data generated by the above-said (c) and, therefore, it becomes difficult to infer processing and a secret key by observation of the waveform of current consumption. See page 10, lines 12-14 and page 84, lines 7-12 of the present specification (in the specification, "f" of claim 1 corresponds to the claimed "OP1").

Turning to the Office Action, the Examiner, on page 10, points to page 21, lines 1-12 of the specification to support his interpretation of the AAPA. This passage describes as AAPA that

> data to be processed is first transformed by using data for disturbance. The transformed data is then processed. Finally, a result of the processing is subjected to inverse transformation by using the data for disturbance or by using a result of processing the data for disturbance to produce a value equal to data which will also be obtained as a result of processing the original data. In this way, the degree of correlation between the magnitude of a current consumed during the processing and the original data is lowered, making it difficult to infer the original data by measuring the current consumption.

The Examiner, however, suggests that this passage admits that before the present invention was made, the person of ordinary skill knew of

> an apparatus including a selector for selecting disturbance data; disturbance data processing means performing predetermined processing on the selected disturbance data to generate processed disturbance data; a data transforming means transforming input data by using the selected disturbance data to generate transformed data; a transformed data processing means for performing predetermined processing on the transformed data to generate processed transformed data; and a data inverse transform means for performing inverse transformation processing on the processed transformed data using the processed disturbance data to generate processed data. (emphasis added)

The underlined portions represent subject matter asserted as inventive subject matter, as noted above at b) and c). The rejection thus fails for lack of a prima facie case of unpatentability, the primary "reference" being misinterpreted.

Furthermore, item a) above is neither taught nor suggested by AAPA or Jaffe, which is discussed in more detail below. In this regard, the Applicants have reviewed the Examiner's comment on page 10, lines 15-18, alleging that Jaffe's teaching of "look-up tables" leads the person of ordinary skill in the art to the claimed "table of candidates of disturbance data XI which maintain a constant Hamming weight before and after processing said disturbance data XI with said predetermined processing OP1." The Examiner refers to column 15, line 61 through column 16, line 14, but this passage only peripherally references look-up tables as an alternate function for which Jaffe's method and apparatus might be employed: "It should be apparent to one of skill in the art that the invention may be used to construct other hardware gates in which the Hamming weight of operands and the number of state transitions are independent of the parameters of computation. Examples of alternate functions include, but are not limited to, look-up tables, logic gates (such as XOR,

AND, etc.), equality or assignment operations, subtraction, multiplication, permutations, symmetric cryptographic operations (DES, SHA, IDEA, etc.), and primitives used to construct asymmetric cryptographic operations (such as, but not limited to, modular multiplication). The invention can be applied to perform functions with more than two inputs (such as a three input logic gate, an eight-bit adder, a binary multiplier, an implementation of the DES f function, a floating-point arithmetic unit, a microprocessor core, etc.) It should also be apparent to one skilled in the arts that the invention can be used to construct leak-resistant operations from a variety of other (leaky) basic operations, such as, but not restricted to, XOR, EQU, addition, and table/memory lookup. Balanced Hamming weight bit representations other than the exemplary ones described can be used." (emphasis added) Note that there is no suggestion whatsoever of a table of candidates of disturbance data XI which maintain a constant Hamming weight before and after processing said disturbance data XI with said predetermined processing OP1.

None of the prior art and cited references have the above-said features of claim 1, (a) – (c), even when taken in any combination that would be suggested to the person of ordinary skill in the art.

The currently amended claim 28 recites the following features: (a') a table of candidate pairs of disturbance data XI and disturbance data XO, wherein said disturbance data XI of said candidate pairs maintains a constant Hamming weight before and after processing said disturbance data XI with said predetermined processing OP1, and wherein said disturbance data XO is obtained from processing said disturbance data XI with said predetermined processing OP1, and (b') a selector for selecting said pair of disturbance data XI and XO from said table.

The embodiment of claim 28 also prevents the Hamming weight of data for disturbance from becoming equal to 0 or 8 by using the first disturbance data and the second disturbance data selected by the above-said process (b') and, therefore, it becomes difficult to infer processing and a secret key by observation of the waveform of current consumption. See page 10, lines 12-14 and page 84, lines 7-12 of the present specification (as above, the operation “f” described in the specification corresponds to "OP1" in claim 28).

Accordingly, claim 28 is distinguishable on grounds similar to those argued above with respect to claim 1.

Jaffe

As mentioned above, although the failure of the Examiner to make out a prima facie case of obviousness has been demonstrated, the Applicants wish to re-emphasize the misinterpretation of Jaffe as applied against the claims.

At the outset, the Applicants acknowledge that Jaffe discloses the use of “a constant Hamming weight representation of data in its internal operations." See column 4, lines 56-67 of Jaffe.

However, Jaffe's statement, "uses a constant Hamming weight representation of data" means data having a constant Hamming weight obtained by adding signals thereto. The Applicants assert that such is apparent to the person of ordinary skill who would consider Jaffe's further statement, "A simple constant Hamming weight representation maps 'one' onto the two-digit binary number 10, and 'zero' onto 01" as an example on col. 5, lines 9-11.

That is, Jaffe shows only that the input data is shown in the form of a "constant Hamming weight representation" and does not show "each of two different data in the constant Hamming weight are before and after the predetermined operation, each other".

Not incidentally, the Applicants note that the level of ordinary skill in this art is a determination that must be made by the Examiner before a prima facie case of obviousness can be made out. It is not necessary for the Applicants to do so to prove patentability, and thus any suggestion of mere “conjecture” by the Examiner should be reviewed.

Returning to the discussion re Jaffe, both of the disturbance data XI and the second disturbance data XO generated by the present invention (see (a) – (c) above) have the following relationship: The second disturbance data XO is obtained by applying the processing OP1 (in specification, shown by "f") on the first disturbance data XI.

This relationship between the first disturbance data XI and the generated second disturbance data XO makes the following "transforming" and "un-transforming":

transforming input data D1 by using the first disturbance data XI to transformed data H1,

transforming transformed data H1 by carrying out processing OP1 to processed transformed data H2, and

“un-transforming” processed transformed data 2 by carrying out inverse-transformation processing OP2 using the second disturbance data XO to processed data D2.

Jaffe does not teach that two different data have the constant Hamming weight as each other before and after the predetermined operation. Therefore, Jaffe fails to show or suggest that for which it is applied in the obviousness rejection, and therefore no combination with AAPA can be said to render claims 1 and 28 unpatentable.

It should be noted that, in the present invention, the first disturbance data selected by the above-said process (b) and the second disturbance data generated by the above-said (c) are used. However, these first and second disturbance data are not obtained by using any combination of the first and second disturbance data of AAPA and "a constant Hamming weight representation" assertedly disclosed by Jaffe.

As argued previously, if the first and second disturbance data of Applicant admitted prior art are given "a constant Hamming weight representation" according to Jaffe, the second disturbance data computed by using the operation f (OP1) on the first disturbance data of AAPA cannot guarantee its Hamming weight not to become 0 or 8. At these values, the data may be inferred. This, of course, is an objective of the presently-claimed invention and must flow from any combination asserted against the claims, because the claims set forth embodiments that ensure that the Hamming weight will not be 0 or 8, and any different result cannot therefore be the invention. Accordingly, the combination of the cited references does not disclose or suggest the present invention.

Furthermore, Jaffe's process using "a constant Hamming weight representation" does not lead to the processed data D2 of the present invention. That is, if one were to hypothetically attempt to transform input data D1 by using first

disturbance data Xi to generate transformed data H1, transform transformed data H1 by carrying out processing to obtain processed transformed data H2, and "un-transform" processed transformed data H2 by using the second disturbance data XO, processed data corresponding to D2 according to the present invention would not be produced. This is apparent in that, if one were to apply Jaffe's "constant Hamming weight representation" to each of the first disturbance data Xi and the second disturbance data Xo of AAPA, the result would not be that the above-said two data have the same, constant Hamming weight both before and after the predetermined operation

In view of the foregoing amendments and remarks, the Applicants request reconsideration of the rejection and allowance of the claims.

To the extent necessary, the Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Brundidge & Stanger, P.C., Deposit Account No. 50-4888 (referencing attorney docket no. NIT-295).

Respectfully submitted,

BRUNDIDGE & STANGER, P.C.

/Daniel J. Stanger/
Daniel J. Stanger
Registration No. 32,846

DJS/sdb
(703) 684-1470